AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) Mobile telephone handset, ~~comprises~~ comprising:

- a storage support which is secured against fraudulent access, which stores the IMEI of the handset;

- a connector for a secure electronic module, which is associated with an operator;

- a handset operating system, which controls authentication of the IMEI storage support by a secure electronic module which is connected to the aforementioned connector, in order to establish a secure communication channel between the storage support and the module and transmission of the IMEI over the secure channel to the secure electronic module.

2. (Previously Presented) Mobile telephone handset according to claim 1, wherein the operating system controls the transmission of the IMEI to a mobile telephone operator by means of a secure OTA channel.

3. (Previously Presented) Handset according to claim 1, wherein it comprises a secure electronic module associated with the operator connected to the connector.

4. (Previously Presented) Handset according to claim 3, wherein the secure electronic module is a UICC.

5. (Previously Presented) Handset according to claim 3, wherein the operating system controls the authentication of the secure module by the storage support.

6. (Previously Presented) Handset according to claim 5, wherein the secure electronic module and the storage support store encryption keys that are adapted to securing the secure communication channel.

7. (Previously Presented) Handset according to claim 3, wherein the secure module blocks the use of the handset when a false IMEI is detected.

8. (Currently Amended) Method of securing the IMEI of a mobile telephone handset comprising the following steps:

- authenticating a secure storage support ~~by memorising its~~ that stores said IMEI, by a secure electronic module associated with the operator and inserted in a connector of the handset, in order to establish a secure channel between the storage support and the secure module;

- transmitting the IMEI from the storage support to the secure module over the secure channel.

9. (Previously Presented) Method according to claim 8, wherein the secure module also transmits the IMEI to a mobile telephone operator over a secure OTA channel.

10. (Previously Presented) Method according to claim 9, wherein the operator compares the IMEI with a black list of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.

11. (Previously Presented) Method according to claim 8, wherein the secure module blocks the use of the handset when a false IMEI is detected.

12. (Previously Presented) Handset according to claim 4, wherein the operating system controls the authentication of the secure module by the storage support.

13. (Previously Presented) Handset according to claim 4, wherein the secure module blocks the use of the handset when a false IMEI is detected.

14. (Previously Presented) Handset according to claim 5, wherein the secure module blocks the use of the handset when a false IMEI is detected.

15. (Previously Presented) Handset according to claim 6, wherein the secure module blocks the use of the handset when a false IMEI is detected.

16. (Previously Presented) Method according to claim 9, wherein the secure module blocks the use of the handset when a false IMEI is detected.

17. (Previously Presented) Method according to claim 10, wherein the secure module blocks the use of the handset when a false IMEI is detected.